

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2002年11月14日 (14.11.2002)

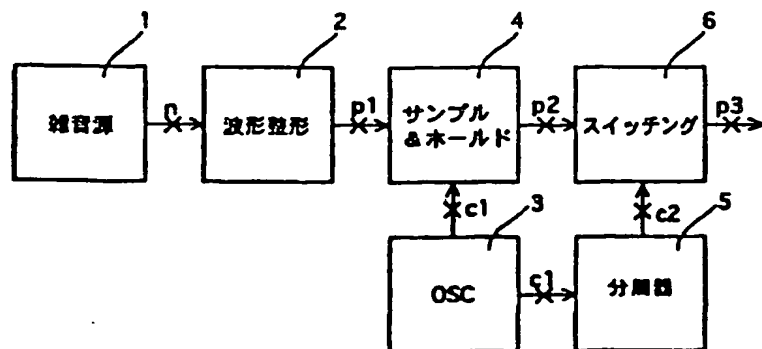
PCT

(10) 国際公開番号
WO 02/091167 A1

- (51) 国際特許分類⁷: G06F 7/58 (74) 代理人: 社本 一夫, 外 (SHAMOTO, Ichio et al.): 〒100-0004 東京都千代田区大手町二丁目2番1号新大手町ビル206区ユアサハラ法律特許事務所 Tokyo (JP).
- (21) 国際出願番号: PCT/JP02/03075
- (22) 国際出願日: 2002年3月28日 (28.03.2002)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2001-163428 2001年4月24日 (24.04.2001) JP
- (71) 出願人 (米国を除く全ての指定国について): 株式会社三技協 (SANGIKYO CORPORATION) [JP/JP]: 〒224-0053 神奈川県横浜市都筑区池辺町4509 Kanagawa (JP). 株式会社サンテクト (SANTEKUTO CORPORATION) [JP/JP]: 〒228-0829 神奈川県相模原市北里2-17-27 Kanagawa (JP).
- (81) 指定国 (国内): AE, AG, AI, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GI, GM, GR, GU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.
- (84) 指定国 (広域): ARIPO 特許 (GI, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- (72) 発明者: および
- (75) 発明者/出願人 (米国についてのみ): 三田 二三夫 (MITA, Fumio) [JP/JP]: 〒228-0829 神奈川県相模原市北里2-17-27 Kanagawa (JP). 渥美 治 (ATSUMI, Osamu) [JP/JP]: 〒228-0802 神奈川県相模原市上鶴間2-8-38 Kanagawa (JP).
- 添付公開書類:
— 国際調査報告書
- 2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: RANDOM NUMBER GENERATOR

(54) 発明の名称: 乱数発生装置



1...NOISE SOURCE

2...WAVEFORM SHAPING

4...SAMPLE & HOLD

5...FREQUENCY DIVIDER

6...SWITCHING

(57) Abstract: A random noise n having no periodicity generated from a noise source (1) is inputted to a waveform shaper circuit (2) to generate a random pulse wave $p1$ which is then inputted, together with a clock $c1$ from an oscillator (3), to a sample & hold circuit (4) thus generating a binary pulse train $p2$ of constant period. The binary pulse train $p2$ and the clock $c1$ are fed to a frequency divider (5) to produce a 1/2 frequency division clock $c2$ which is then inputted to a switching circuit (6) in order to invert the polarity of the binary pulse train $p2$ every other period thus producing a smooth binary pulse train $p3$ where the balance of occurrence of 1/0 codes is made smooth.



(57) 要約:

本発明は、雑音源 1 が発生する周期性のないランダム雑音 n を波形整形回路 2 に入力してランダムパルス波 p_1 を生成し、次に、ランダムパルス波 p_1 と発振器 3 のクロック c_1 をサンプル&ホールド回路 4 に入力して一定周期の 2 値パルス列 p_2 を生成し、その 2 値パルス列 p_2 とクロック c_1 を分周器 5 で $1/2$ に分周した $1/2$ 分周クロック c_2 をスイッチング回路 6 に入力して 2 値パルス列 p_2 の極性を 1 周期おきに反転させ、 $1/0$ 符号の出現バランスを平滑化した平滑 2 値パルス列 p_3 を出力する。

(51)Int.Cl.

G 0 6 F 7/58

識別記号

F I

G 0 6 F 7/58

デモコード*(参考)

A

審査請求 未請求 請求項の数3 O L (全 10 頁)

(21)出願番号 特願平11-104743

(22)出願日 平成11年4月13日(1999. 4. 13)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(71)出願人 599050826

文部省統計数理研究所長

東京都港区南麻布4-6-7

(72)発明者 吉田 健治

神奈川県秦野市堀山下1番地 株式会社日

立製作所汎用コンピュータ事業部内

(74)代理人 100080001

弁理士 筒井 大和

最終頁に続く

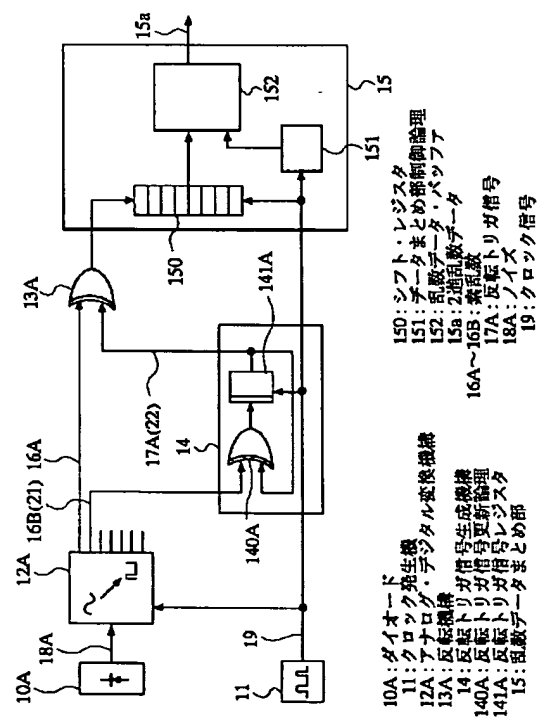
(54)【発明の名称】 乱数生成装置

(57)【要約】

【課題】 ランダム性のある物理現象を利用したハードウェア生成による乱数生成装置において、高速な乱数生成速度と、高い乱数性を同時に実現する。

【解決手段】 ダイオード10Aの出力するノイズ18Aを、アナログ・デジタル変換機構12Aでデジタル・データに変換し、デジタル・データのうちの何ビットかを素乱数16A、16B、...として取り出す。反転トリガ信号生成機構14で0と1の出現比率が均等な反転トリガ信号17Aを生成し、反転機構13Aにて素乱数16Aとの排他的論理和をとり2進乱数データ15aの乱数として乱数データまとめ部15から出力する。反転トリガ信号生成機構14の一手段として素乱数16Bを利用し、素乱数16Bが1の時に直前の反転トリガ信号17Aの反転した値を反転トリガ信号17Aとして反転機構13Aに入力する。

図 3



【特許請求の範囲】

【請求項1】 時間軸方向に規則性のない物理量を発生する物理量発生手段と、前記物理量を2ビット以上の第1のデジタルデータに変換するデータ変換手段と、前記第1のデジタルデータの少なくとも一部を乱数データとして外部に出力する外部出力インタフェースと、を含む乱数生成装置であって、

0と1が変化しながらほぼ同じ比率で現れる反転トリガ信号を生成する反転トリガ信号生成手段と、

前記データ変換手段と前記外部出力インタフェースとの間に設けられ、前記第1のデジタルデータの少なくとも一部のビットと、前記反転トリガ信号との排他的論理和をとり、前記第1のデジタルデータの代わりに第2のデジタルデータとして前記外部出力インタフェースに出力するデータ反転手段と、

を含むことを特徴とする乱数生成装置。

【請求項2】 請求項1記載の乱数生成装置において、前記反転トリガ信号生成手段は、任意の乱数発生手段から時系列に入力されるデジタルの乱数データと、自身の出力との排他的論理和をとり、前記反転トリガ信号として出力する反転トリガ更新論理と、前記反転トリガ更新論理から出力される前記反転トリガ信号をラッチして前記データ反転手段および前記反転トリガ更新論理に出力する反転トリガ信号ラッチ手段とを含むことを特徴とする乱数生成装置。

【請求項3】 請求項1または2記載の乱数生成装置において、

前記反転トリガ信号生成手段の前記反転トリガ更新論理に入力される前記乱数データとして、前記第1のデジタルデータの一部を用いる構成、

前記物理量発生手段および前記データ変換手段の組み合わせを、デジタルデータを前記データ反転手段に入力する組と、前記デジタルデータを前記乱数データとして前記反転トリガ信号生成手段の前記反転トリガ更新論理に入力する組の2系統設ける構成、

前記物理量発生手段および前記データ変換手段の組み合わせを、前記デジタルデータを前記データ反転手段に入力する組と、前記デジタルデータを前記乱数データとして前記反転トリガ信号生成手段の前記反転トリガ更新論理に入力する組の2系統設け、前記反転トリガ更新論理に前記乱数データとして入力される前記デジタルデータとして、互いに他の前記デジタルデータを用いる構成、

前記反転トリガ更新論理に入力される前記乱数データとして、ソフトウェア生成乱数を用いる構成、

のいずれかの構成を含むことを特徴とする乱数生成装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、乱数生成技術に関

し、特に、ハードウェアによって乱数を生成する場合における生成過程の高速化および高い乱数性の実現等に好適な乱数生成技術に関する。

【0002】

【従来の技術】乱数は、様々なシミュレーションにおける不確定要素や、無作為抽出のための選択手段、暗号化技術の鍵生成などの分野で利用される。たとえば、風洞実験のシミュレーションで与える風は均質な物でなく、風向、風速、圧力などいくつかのパラメータに不確定さが必要になる。また、数学の世界では、モンテカルロ法など乱数を計算に使用する。こうした乱数に、多くはソフトウェア生成の乱数が用いられている。

【0003】しかし、ソフトウェア乱数は疑似乱数と呼ばれるように、出力した乱数列に一定の規則性があり、結果に誤った指向性が出たり、結果の収束に影響したりすることがある。

【0004】ハードウェア生成による乱数は、乱数源にランダム性があり、時間方向に規則性の無い物理現象を選ぶことによって、ソフトウェア乱数の様な規則性を無くすることができる。たとえば、仁木直人「工学的乱数発生」統計数理研究所彙報 第27巻 第1号 1980

115-131、等の文献にも記載されているよう

に、過去のハードウェア乱数生成の乱数源に選ばれたランダム性のある物理現象には、コバルト-60の放射線量、セシウム-137の崩壊によるガンマ線放射、トランジスタの熱雑音、ダイオードの熱雑音、ネオン放電管からの雑音等がある。

【0005】乱数への加工方法として2種類の例を示す。ひとつは、前記の放射線量や、ノイズをパルス化したものを、一定時間計数した結果が偶数であるか奇数であるかで2進1桁乱数を生成する方法である。もうひとつは、ランダム性のある物理現象のうちノイズが得られるものを利用し、得られたノイズをアナログ・デジタル変換し、出力の何桁かを乱数として利用する方法である。後者の例として、特開平6-314188号公報の技術では、導線上のノイズをアナログ・デジタル変換し、乱数を生成している。

【0006】

【発明が解決しようとする課題】2進乱数の乱数性の評価の尺度には、(1)0と1の出現する比率が等しいこと、(2)ある桁の0と1の出現する比率が、前に出現した別の桁のパターンに左右されないこと、がある。

【0007】本明細書の中で(1)は「0と1の出現比率が等しい」、(2)は「乱数列の規則性がない」と表現する。(2)について例を挙げると、00と続いた後の0と1の出現する比率が1:3となる場合「規則性がある」わけで、それだけ「乱数性が悪い」となる。

(1)(2)はいずれも統計的な評価のため、評価対象の母集団が大きいほど正しく評価でき、母集団が小さいケースでは常に成り立つものではない。

【0008】従来の技術で説明した、一定時間におけるある物理現象を計数することによる乱数生成装置は、計数した値が充分大きくなる時間を必要とする。極端な例を挙げると、一定時間計数した結果が0から1程度だとして、ほとんどの場合0だとすると偶数と奇数の出現比率が著しく不均等なために、出力する乱数に指向性が出てしまう。たとえば100を中心に50から150の値を計数できるような、充分大きく、充分ばらつきのある値が計数できる時間を取れば、偶数と奇数の出現比率の不均衡が無視できる様になる。しかし、出現比率の差を小さくするために計数時間を大きくとれば、乱数の生成速度は反比例して遅くなる。前述した100を中心に50から150の値を計時できるような時間をとると、理論上回路の動作周波数の1/150以下、おそらくは1/200から1/300程度の乱数生成速度しか得られない。

【0009】従来の技術で説明したもう一方の、ランダム性のあるノイズをアナログ・デジタル変換し、出力の何桁かを乱数として利用する方法では、アナログ・デジタル変換機構の回路上のくせによって各桁の0と1の出現比率が均等にならない場合が考えられる。ノイズをアナログ・デジタル変換する方法では物理現象を計数する方法に比べて、回路の動作周波数とほぼ同等の乱数生成速度を得ることができる。しかし、回路内の主にアナログ・デジタル変換機構内部の信号が0から1、1から0に変化する速さの違いやスレッシュールド電圧の違いを始め、ノイズ源のダイオードから誘導される電源線、接地線、信号線へのノイズなど、回路特有のくせにより、実際のノイズの電圧値とアナログ・デジタル変換機構が出力するデジタル・データの値に誤差が生じる。たとえば、変換前のノイズがxからx+1の中間の電圧であった場合に、アナログ・デジタル変換機構の出力する結果がxよりx+1を出力する確率が多いと、出力する各桁の0と1の出現比率に偏りが生じてしまい、これを乱数とすると0と1の出現比率に偏りがある乱数になる。回路のくせは、回路を構成する素子の特性、温度、供給電*

$$b = 4 \times a^3 - 6 \times a^2 + 3 \times a$$

【0014】となる。実際aが0.5近辺の値を取った場合、bはどうか計算して図7に示す。

【0015】a、bの0.5との差分と0.5との比率を以下では、乱数の偏差と表現することとする。図7を見ると分かるように、素乱数の偏差が1%の場合で、出力した乱数の偏差は 10^{-8} と非常に小さくできる。

【0016】本発明で採用している反転トリガ信号生成機構は、反転トリガ信号生成機構に入力する素乱数が1の時に同期して反転トリガ信号を0から1又は1から0へ切り替え、素乱数が0の時は反転トリガ信号を変化させない。素乱数の乱数列には規則性が無いため、生成した反転トリガ信号は0と1の出現比率は理論上均等になる。図6は、素乱数21とこの素乱数21を元に生成し

* 圧、動作周波数など、様々な条件に左右され、回路の改善で偏りを無くすることは困難である。

【0010】本発明の目的は、ハードウェアによって乱数列を生成する乱数生成技術において、高速な乱数生成速度と、乱数列に規則性が無く、均質な0と1の出現比率を同時に実現することにある。

【0011】

【課題を解決するための手段】本発明では、物理量発生手段から得られる時間軸方向に規則性のない物理量をデジタル量に変換するアナログ・デジタル変換機構の出力するデジタル・データのあるビット（以下、素乱数と呼ぶ）を、反転トリガ信号と排他的論理和を取って乱数とする。反転トリガ信号は、0と1の出現比率が1:1となり、できるだけ規則性の無いものを生成する。この方法により、乱数として0を出力する場合に、アナログ・デジタル変換機構が0を出力している場合と1を出力している場合とどちらの場合もあり、乱数として1を出力する場合も同じくアナログ・デジタル変換機構が0を出力している場合と1を出力している場合とどちらの場合もあるため、アナログ・デジタル変換機構の回路の特有のくせが出力に与える影響を無くすることができる。

【0012】また、反転トリガ信号に規則性がある場合にも、出力した乱数列の規則性は改善される。反転トリガ信号の規則性を、0が出現した後に0と1が出現する確率を $a : 1 - a$ ($0 < a < 1$) とすると、0と1の出現比率が1:1なので、1が出現した後の0と1が出現する確率は $1 - a : a$ となる。素乱数の0と1の出現比率の偏りも簡単のため、同じく $a : 1 - a$ として、aの値が0.5からずれた場合、出力する乱数列の規則性にどの程度の影響が出るか計算してみる。出力する乱数列の規則性は、前記の表現と同じように0が出現した後の0と1が出現する確率を $b : 1 - b$ 、1の出現した後の0と1の出現する確率を $1 - b : b$ と表現する。すると、

【0013】

【数1】

【式1】

た反転トリガ信号22の関係の一例を信号の波形で表している。信号の波形が上にある時の信号の値が1を表し、信号の波形が下にある時の信号の値が0を表す。素乱数21は0の出現比率が高いが、反転トリガ信号22は0と1の出現比率はほぼ等しくなっているのがわかる。

【0017】反転トリガ信号の規則性は、素乱数の偏差と同程度の影響がある。なぜなら、規則性の一つである0の後1になる確率、1の後0になる確率は、素乱数の1が出現する確率に等しいからである。しかし、後述する実施の形態で見てみた場合、うまく回路を構成することによって、アナログ・デジタル変換機構の出力のうち、偏差が1~2%程度の素乱数を得ることが可能であ

り、前述したように、この程度の偏差が出力の偏差に与える影響は非常に小さくできる。また、規則性が存在するソフトウェア乱数と組み合わせて乱数を生成しても、乱数性の高い乱数が得られる。

【0018】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照しながら詳細に説明する。

【0019】図1は、本発明の一実施の形態である乱数生成装置の構成の一例を示す概念図である。本実施の形態の乱数生成装置は、経時的に不規則なノイズ18Aを発生するダイオード10A、ノイズ18Aを素乱数16A～16Dのディジタルデータに変換するアナログ・デジタル変換機構12A、反転トリガ信号17A～17Dを生成する反転トリガ信号生成機構14、アナログ・デジタル変換機構12Aおよび反転トリガ信号生成機構14にクロック信号19を供給するクロック発生機構11、乱数を使用する外部の任意の情報処理装置等との間のインタフェースを提供する乱数データまとめ部15、を含んでいる。

【0020】すなわち、ダイオード10Aが出力するノイズ18Aをアナログ・デジタル変換機構12Aに入力する。アナログ・デジタル変換機構12Aの出力する素乱数のうちの素乱数16A～16Dを反転機構13A～13Bのデータ入力に、反転トリガ信号生成機構14の出力する反転トリガ信号17A～17Bは、反転機構13A～13Bの反転トリガ入力に接続する。反転機構の13Aの出力は、乱数データまとめ部15に接続する。

【0021】このような構成の本実施の形態の乱数生成装置の動作としては、まず、アナログ・デジタル変換機構12Aは、クロック信号19に同期して、ノイズ18Aの電圧をデジタル・データに変換する。このデジタル・データから素乱数16A～16Dを取り出す。反転機構13A～13Bは、素乱数16A～16Dと反転トリガ信号生成機構14の出力する反転トリガ信号17A～17Bの排他的論理和を出力し、乱数データまとめ部15に送る。乱数データまとめ部15は、外部からの要求でデータを取り出しやすいように加工し、2進乱数データ15aとして出力する。素乱数のビット数と反転機構の数は同じだが、反転トリガ信号はそれと異なっても構わない。

【0022】図2は、前述の図1に例示された乱数生成装置のより具体的な変形例を示す概念図である。すなわち、この図2の構成例は、図1の反転トリガ信号生成機構14の実現方法の一つを提示している。

【0023】この図2の構成では、反転トリガ信号生成機構14は、複数の反転トリガ信号更新論理140A～140Bおよび反転トリガ信号レジスタ141A～141Bを含んでいる。そして、アナログ・デジタル変換機構12Aの出力する素乱数のうち反転機構13A～13Bに直接送られなかった素乱数16E～16Fを、それ

ぞれ反転トリガ信号生成機構14内の反転トリガ信号更新論理140A～140Bに接続する。反転トリガ信号更新論理140A～140Bの出力はそれぞれ反転トリガ信号レジスタ141A～141Bに接続し、反転トリガ信号レジスタ141A～141Bの出力する反転トリガ信号17A～17Bは、反転機構13A～13Bのいずれかの反転トリガ入力と、それぞれ反転トリガ信号更新論理140A～140Bに接続する。

【0024】この図2の変形例の動作としては、反転トリガ信号更新論理140Aは、反転トリガ信号17Aと素乱数16Eの排他的論理和を出力する。反転トリガ信号レジスタ141Aは、クロック信号19に同期して、保持する値を反転トリガ信号更新論理140Aの出力に置き換える。反転トリガ信号更新論理140Bと反転トリガ信号17B、素乱数16F、反転トリガ信号レジスタ141Bの動作も同様である。このようにして、反転トリガ信号17A、17Bを生成する以外は図1の説明と同様である。

【0025】図3は、本発明の他の実施の形態である乱数生成装置の構成の一例を示す概念図である。この図3の構成の場合、アナログ・デジタル変換機構12Aは8ビット出力のものとし、アナログ・デジタル変換機構12Aの出力する8個の素乱数のうち1個の素乱数16Aを1個の反転機構13Aのデータ入力に、別の1個の素乱数16Bを反転トリガ信号生成機構14内の1個の反転トリガ信号更新論理140Aに接続する。反転トリガ信号更新論理140Aの出力は反転トリガ信号レジスタ141Aに接続し、反転トリガ信号レジスタ141Aの出力する反転トリガ信号17Aは、反転機構13Aの反転トリガ入力と、反転トリガ信号更新論理140Aの入力側に接続する。

【0026】反転機構13Aの出力は、乱数データまとめ部15内のシフト・レジスタ150に接続し、シフト・レジスタ150の出力は、乱数データまとめ部15内の乱数データ・バッファ152に接続する。乱数データまとめ部15内のデータまとめ部制御論理151の出力は、乱数データ・バッファ152に接続する。クロック発生機構11が出力するクロック信号19は、アナログ・デジタル変換機構12Aと、反転トリガ信号レジスタ141Aと、シフト・レジスタ150と、データまとめ部制御論理151に接続する。

【0027】この図3の構成の乱数生成装置の動作としては、まず、アナログ・デジタル変換機構12Aは、クロック信号19に同期して、ノイズ18Aの電圧を8ビットのデジタル・データに変換する。このデジタル・データから2個の素乱数16Aと16Bを取り出す。反転トリガ信号更新論理140Aは、反転トリガ信号17Aと素乱数16Bの排他的論理和を出力する。反転トリガ信号レジスタ141Aは、クロック信号19に同期して、保持する値を反転トリガ信号更新論理140Aの出

力に置き換える。反転機構13Aは、素乱数16Aと反転トリガ信号17Aの排他的論理和を出力し、シフト・レジスタ150に入力する。シフト・レジスタ150は、8ビットのシフト・レジスタで、クロック信号19に同期してシフト動作と、反転機構13Aの出力の取り込みを行う。シフト・レジスタ150は、8ビット幅の出力を乱数データ・バッファ152に送り、データまとめ部制御論理151は、クロック信号19に同期して、8サイクルに1回、乱数データ・バッファ152に書き込み指示を行う。乱数データ・バッファ152は、書き込み指示を受けた時のシフト・レジスタ150からのデータ(2進乱数データ15a)を記憶する。また乱数データ・バッファ152は、外部からの読み出し要求に対して、2進乱数データ15aの書き出しと、書き出した2進乱数データ15aの消去を行う機能と、たとえばPCI等の汎用バス等に対する接続インターフェースを有し、8ビットの乱数データ(2進乱数データ15a)を外部の任意の装置等に供給することができる。

【0028】図4は本発明の他の実施の形態である乱数生成装置の構成の一例を示す概念図である。この図4の構成では、反転トリガ信号生成機構14に対する素乱数の入力手段として専用のダイオード10Bおよびアナログ・デジタル変換機構12Bを設けた構成となっている。

【0029】すなわち、反転機構13A～13Bに接続する素乱数16A～16Bに、ダイオード10Aが出力するノイズ18Aをアナログ・デジタル変換機構12Aがアナログ・デジタル変換した出力を用い、反転トリガ信号生成機構14内の反転トリガ信号更新論理140A～140Bに接続する素乱数16E～16Fに、ダイオード10Bが出力するノイズ18Bをアナログ・デジタル変換機構12Bがアナログ・デジタル変換した出力を用いている。

【0030】この図4の構成では、複数のダイオード10Aおよび10Bと、アナログ・デジタル変換機構12Aおよび12Bの組合せを2系統用意したことにより、複数の反転機構13Aおよび13Bに輸入される素乱数16Aおよび16Bと、反転トリガ信号17Aおよび17Bとの間の相関を無くすることが可能となり、最終的に乱数データまとめ部15から出力される2進乱数データ15aにおいてより高い乱数性を実現することができる。

【0031】図5は、図4に例示した本発明の乱数生成装置の変形例を示す概念図である。この図5の構成では、ダイオード10Aおよびアナログ・デジタル変換機構12Aと、ダイオード10Bおよびアナログ・デジタル変換機構12B、の2系列の素乱数16A、素乱数16B、および素乱数16G、素乱数16H、に対して、対応した反転機構13A、13Bおよび反転機構13C、13Dを設けるとともに、反転機構13A、13B

および反転機構13C、13Dの各々に対する反転トリガ信号17Aおよび反転トリガ信号17Bが、互いに他方のアナログ・デジタル変換機構12Bおよび12Aから発生された素乱数16Eおよび素乱数16Jにてクロスして生成される構成としたものである。

【0032】すなわち、ダイオード10Aが出力するノイズ18Aを8ビット出力のアナログ・デジタル変換機構12Aに入力する。ダイオード10Bが出力するノイズ18Bを8ビット出力のアナログ・デジタル変換機構12Bに入力する。アナログ・デジタル変換機構12Aの出力する8個の素乱数のうち1個の素乱数16Aを反転機構13Aのデータ入力に、1個の素乱数16Bを反転機構13Bのデータ入力に、1個の素乱数16Cを反転トリガ信号生成機構14内の反転トリガ信号更新論理140Bに接続する。アナログ・デジタル変換機構12Bの出力する8個の素乱数のうち1個の素乱数16Gを反転機構13Cのデータ入力に、1個の素乱数16Hを反転機構13Dのデータ入力に、1個の素乱数16Jを反転トリガ信号生成機構14内の反転トリガ信号更新論理140Aに接続する。反転トリガ信号更新論理140Aの出力は反転トリガ信号レジスタ141Aに接続し、反転トリガ信号レジスタ141Aの出力する反転トリガ信号17Aは、反転機構13A、13Bの反転トリガ入力と、反転トリガ信号更新論理140Aの入力側に接続する。反転トリガ信号更新論理140Bの出力は反転トリガ信号レジスタ141Bに接続し、反転トリガ信号レジスタ141Bの出力する反転トリガ信号17Bは、反転機構13C、13Dの反転トリガ入力と、反転トリガ信号更新論理140Bに接続する。反転機構の13A、13B、13C、13Dの出力は、乱数データまとめ部15に接続する。クロック発生機構11が出力するクロック信号19は、アナログ・デジタル変換機構12A、12Bと、反転トリガ信号レジスタ141A、141Bと、乱数データまとめ部15に接続する。前述の図3の実施の形態と異なるのは、(1)ダイオードとアナログ・デジタル変換機構が2個ずつあること、(2)1個のアナログ・デジタル変換機構に対して、2個の反転機構を備え、2個の素乱数を1個ずつ、それぞれの反転機構に輸入していること、(3)アナログ・デジタル変換機構12Aの出力する素乱数16A、16Bの接続する、反転機構13A、13Bに輸入する反転トリガ信号17Aは、もう一方のアナログ・デジタル変換機構12Bの出力する素乱数16Jを利用して更新し、アナログ・デジタル変換機構12Bの出力する素乱数16G、16Hの接続する、反転機構13C、13Dに輸入する反転トリガ信号17Bは、もう一方のアナログ・デジタル変換機構12Aの出力する素乱数16Eを利用して更新していること、である。

【0033】乱数データまとめ部15内では図3の実施の形態と同じように、外からの読み出し要求に応答でき

10

20

30

40

50

るようにデータの形を整え記憶する。本実施の形態では、ダイオードから乱数データまとめ部15の前までの回路を倍にし、利用する素乱数も倍にして乱数生成速度の性能を向上し、しかも反転トリガ信号17A、反転トリガ信号17Bを更新するための素乱数16J、16Eを交換しあうことで、素乱数16A、16Bおよび素乱数16G、16Hと、反転トリガ信号17A、17Bを別系統の乱数源から生成するため、反転機構13A、13Bおよび反転機構13C、13Dのデータ入力(素乱数16A、16Bおよび素乱数16G、16H)、反転トリガ信号17A、17Bの間の予期せぬ相関から規則性が生じることを回避している。

【0034】なお、上述の図2～図5における乱数生成装置の構成例では、反転トリガ信号生成機構14において反転トリガ信号17A、17B等を生成するための素乱数は、ダイオード10A、10Bおよびアナログ・デジタル変換機構12A、12B等を用いてハードウェア的に得られた素乱数を用いているが、これに限らず、図8に例示されるように、ソフトウェア乱数生成装置30において、たとえばM系列法、合同式法等の所望のアルゴリズムを用いたソフトウェアにて生成されたソフトウェア素乱数30aを、素乱数16B、16E、16F、16J、等の代わりに用いても、同様に、得られる2進乱数データ15aの生成速度が高速で、乱数列に規則性が無く、均質な0と1の出現比率を同時に実現することが可能になる。この場合、ソフトウェア乱数生成装置30は、たとえば図示しないマイクロプロセッサや、乱数を生成するためのソフトウェア等が格納されるROM、RAM等を備えた一般的に情報処理装置で構成することができる。

【0035】さらに、図9のフローチャートに例示されるように、反転トリガ信号生成機構14および反転機構13A～13D等で行われる素乱数16A、16B、16H、16G等の反転処理を、当該素乱数16A～16Gを利用する任意の情報処理装置の内部で、ソフトウェア的に行わせることもできる。この場合、物理現象を利用する乱数発生機構としては、本発明の上述の実施の形態で例示したダイオード10A、アナログ・デジタル変換機構12A、乱数データまとめ部15等で構成された、素乱数16A等をそのまま外部に出力する構成の物理乱数生成装置を用いることができる。

【0036】すなわち、任意の情報処理装置において、物理乱数生成装置から得られる素乱数16Aを用いるプログラムでは、前処理として、図9のフローチャートに例示された以下のような処理を行うことで乱数性の向上を達成することができる。

【0037】すなわち、まず、物理乱数生成装置から得られた素乱数16A(2進ハードウェア乱数)を、整数変数HRに格納する(ステップ201)。

【0038】次に、自前のソフトウェアによる乱数発生

ルーチンから2進ソフトウェア乱数を生成して整数変数SRに格納する(ステップ202)。

【0039】整数変数SRの各ビットを指定するためのビット指標変数nを0に初期化する(ステップ203)。ただし、SR[n=0]はLSBを示す。

【0040】次に、SRのLSB(SR[n=0])を“0”との排他的論理和をとって更新する(ステップ204)。

【0041】その後、ビット指標変数nをインクリメントして(ステップ205)、ビット位置がSRのMSBを越えたか否かを判定(ステップ206)しながら、SRのMSB方向に隣接する第nビットと第n-1ビットとの排他的論理和をとって当該第nビット位置のビット値を更新する(ステップ207)操作を、MSBまで反復し、このステップ207の操作が終わったら、整数変数HRに格納された2進ハードウェア乱数と、整数変数SRに格納された反転操作後の2進ソフトウェア乱数との間で各ビット毎の排他的論理和をとり、結果を整数変数HRに書き戻す処理(ステップ208)、を行う。

【0042】これにより、整数変数HR内には、結果として、図1の乱数データまとめ部15から得られる2進乱数データ15aと同様に、乱数列に規則性が無く、均質な0と1の出現比率を持つ、2進ハードウェア乱数が得られる。

【0043】この場合には、ソフトウェア的にビット反転処理を行うため、多少、生成速度は犠牲になるが、素乱数16Aを供給する物理乱数生成装置は任意のものを用いることができ、物理乱数を利用する情報処理装置のソフトウェアの側のわずかな変更で、高い乱数性を持つ物理乱数を使用できるようになる、という利点がある。また、生成速度の点も、物理乱数を利用する情報処理装置の実行速度が改善されれば問題にならなくなり、乱数生成の高速性の要求も満たされる。

【0044】以上説明したように、本実施の形態の乱数生成装置では、ハードウェアによる高速な生成速度の乱数生成処理において、0と1の出現比率については均等にでき、素乱数の偏差が最終的に出力される乱数の規則性へ与える影響を少なくすることができる。図7で示したとおり、乱数列の規則性の偏りは、素乱数の0と1の出現比率の偏りが2%の場合で 10^{-1} 以下、1%で 10^{-6} に改善することができる。

【0045】本発明の特許請求の範囲に記載された以外のの特徴を列挙すれば以下の通りである。

【0046】<1> ノイズ源としてのダイオードと、アナログ・デジタル変換機構と、乱数データまとめ部と、クロック発生機構を有し、クロック発生機構が発生するクロック信号を、前記アナログ・デジタル変換機構に接続し、前記ダイオードに逆バイアスをかけた場合のツェナー降伏領域もしくはアバランシェ領域で発生するノイズの電圧を、前記アナログ・デジタル変換機構で前

記クロックに同期して n ビット ($n > 1$) のデジタル・データに変換し、該デジタル・データのうち m ビット ($1 \leq m \leq n$) を乱数データまとめ部に乱数として利用できる形にまとめる乱数生成装置において、データ入力と反転トリガ入力の2個の入力を持つ m 個の反転機構と、反転トリガ信号生成機構を備え、該反転トリガ信号生成機構は、0と1が変化しながらほぼ同じ比率で現れる反転トリガ信号を s 個 ($1 \leq s \leq m$) 生成し、該 s 個の反転トリガ信号を、合計 m 個全ての前記反転機構の反転トリガ入力に1対1もしくは1対多で接続し、前記乱数データまとめ部に送られる直前の m ビットのデジタル・データを該 m 個の反転機構のデータ入力に1対1で接続し、該 m 個の反転機構はデータ入力と反転トリガ入力の排他的論理和を出力し、該出力を、前記アナログ・デジタル変換機構が出力した m 桁のデジタル・データの代わりに前記乱数データまとめ部に送ることを特徴とする乱数生成装置。

【0047】<2> 反転トリガ信号を保持する s 個の反転トリガ信号レジスタと、 s 個の反転トリガ信号更新論理を有し、前記アナログ・デジタル変換機構の出力するデジタル・データのうち s ビットを s 個の該反転トリガ信号更新論理全てに1対1で接続し、該反転トリガ信号更新論理は対応する反転トリガ信号レジスタが保持する反転トリガ信号と前記入力されたデジタル・データとの排他的論理和を出力し、前記反転トリガ信号レジスタに前記クロックを接続し、該反転トリガ信号レジスタが保持している反転トリガ信号を、クロックに同期して前記反転トリガ信号更新論理の出力に置き換え、該反転トリガ信号レジスタの保持している反転トリガ信号を出力することを特徴とする反転トリガ信号生成機構を備える項目<1>記載の乱数生成装置。

【0048】<3> プログラム生成乱数を前記反転トリガ信号として出力する反転トリガ信号生成機構を有する、項目<1>記載の乱数生成装置。

【0049】<4> 前記ダイオードと前記アナログ・デジタル変換機構の組み合わせを、前記反転機構のデータ入力に接続するものと、前記反転トリガ信号更新論理に接続するものを独立して2系統用意することを特徴とする項目<2>記載の乱数生成装置。

【0050】<5> 前記ダイオードと前記アナログ・デジタル変換機構と反転機構の組み合わせを2系統有し、該反転機構の出力を別の反転機構のデータ入力と反転トリガ入力に接続することを特徴とする項目<1>記載の乱数生成装置。

【0051】<6> 時間軸方向に不規則な物理量から2値の素乱数を生成するステップと、0と1が変化しながらほぼ同じ比率で現れる反転トリガ信号を生成するステップと、前記素乱数と前記反転トリガ信号との排他的

論理和をとって2進乱数として出力するステップと、を含むことを特徴とする乱数生成方法。

【0052】以上本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【0053】たとえば、物理量発生手段としては、上述の実施の形態に例示したダイオードに限らず、時間軸方向に不規則な物理量を出力する一般の機器を広く用いることができる。

【0054】

【発明の効果】本発明の乱数生成装置によれば、ハードウェアによって乱数列を生成する乱数生成技術において、高速な乱数生成速度と、乱数列に規則性が無く、均質な0と1の出現比率を同時に実現することができる、という効果が得られる。

【図面の簡単な説明】

【図1】本発明の一実施の形態である乱数生成装置の構成の一例を示す概念図である。

【図2】図1に例示された乱数生成装置のより具体的な変形例を示す概念図である。

【図3】本発明の他の実施の形態である乱数生成装置の構成の一例を示す概念図である。

【図4】本発明の他の実施の形態である乱数生成装置の構成の一例を示す概念図である。

【図5】図4に例示した本発明の乱数生成装置の変形例を示す概念図である。

【図6】素乱数と、この素乱数を元に生成した反転トリガ信号の関係の一例を信号の波形で表した線図である。

【図7】本発明の一実施の形態である乱数生成装置の作用の一例を表形式で例示した説明図である。

【図8】本発明の他の実施の形態である乱数生成装置の構成の一例を示す概念図である。

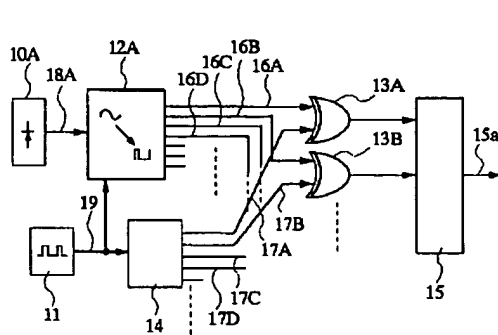
【図9】本発明の乱数生成技術をソフトウェアにて行わせる場合の一例を示すフローチャートである。

【符号の説明】

10A、10B…ダイオード、11…クロック発生機構、12A、12B…アナログ・デジタル変換機構、13A～13D…反転機構、14…反転トリガ信号生成機構、15…乱数データまとめ部、15a…2進乱数データ、16A～16J…素乱数、17A～17D…反転トリガ信号、18A、18B…ノイズ、19…クロック信号、21…素乱数、22…反転トリガ信号、30…ソフトウェア乱数生成装置、30a…ソフトウェア素乱数、140A～140B…反転トリガ信号更新論理、141A～141B…反転トリガ信号レジスタ、150…シフト・レジスタ、151…データまとめ部制御論理、152…乱数データ・バッファ。

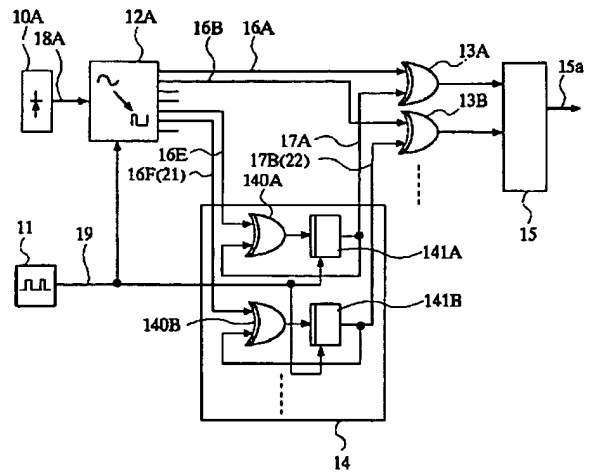
【図1】

図 1



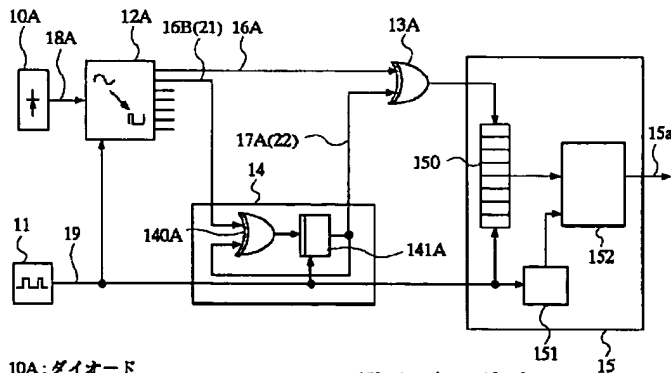
【図2】

図 2



【図3】

図 3



10A: ダイオード
11: クロック発生機構
12A: アナログ・デジタル変換機構
13A: 反転機構
14: 反転トリガ信号生成機構
140A: 反転トリガ信号更新論理
141A: 反転トリガ信号レジスタ
15: 乱数データまとめ部

150: シフト・レジスタ
151: データまとめ部制御論理
152: 乱数データ・バッファ
15a: 2進乱数データ
16A~16B: 素乱数
17A: 反転トリガ信号
18A: ノイズ
19: クロック信号

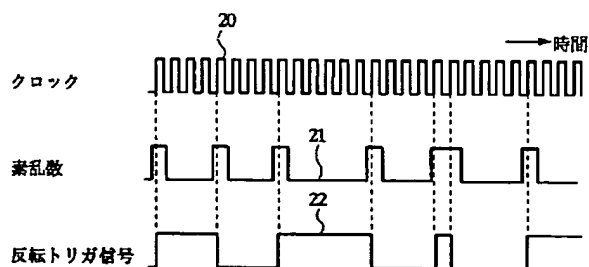
【図7】

図 7

a	b
0.6	0.504
0.55	0.5005
0.54	0.500256
0.53	0.500108
0.52	0.500032
0.51	0.500004
0.505	0.5000005
0.5	0.5

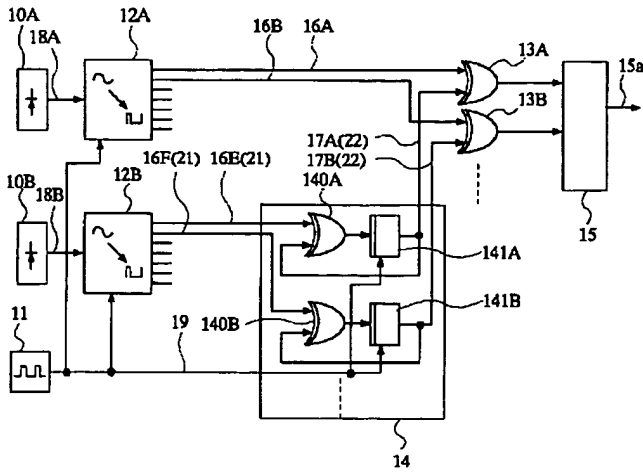
【図6】

図 6



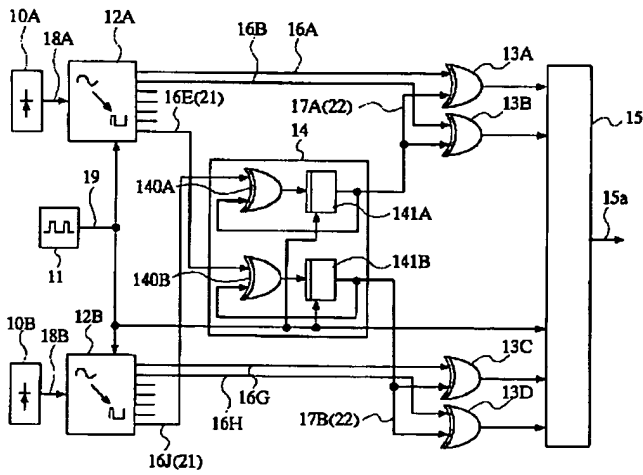
【図4】

図 4



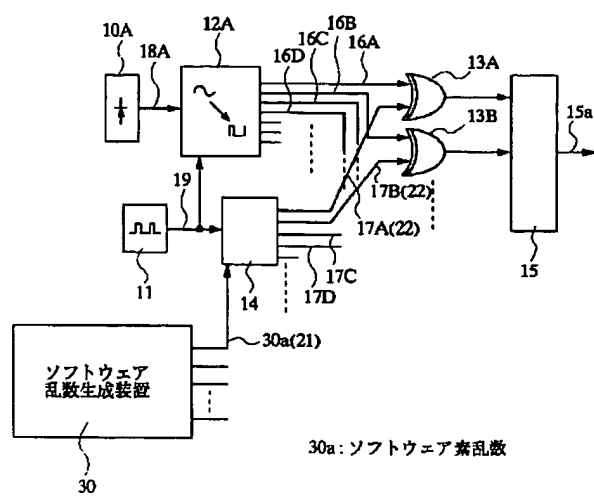
【図5】

図 5



【図8】

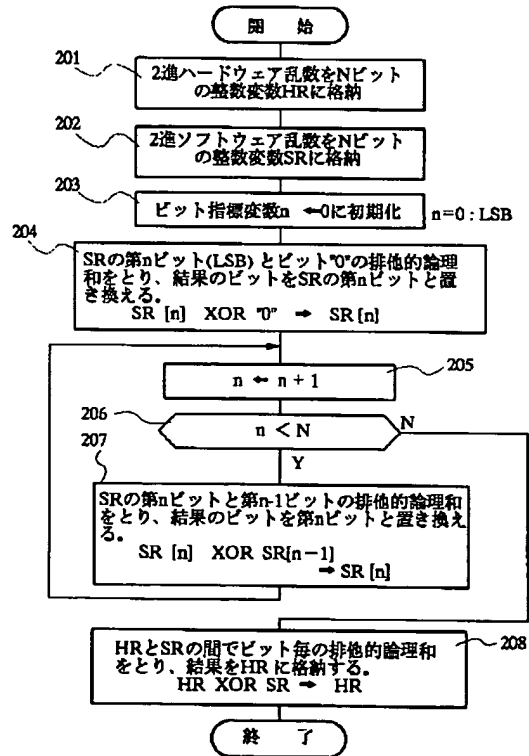
図 8



【図9】

図 9

ハードウェア乱数をソフトウェア的に反転処理する例



フロントページの続き

(72)発明者 田村 義保
東京都港区南麻布4-6-7 統計数理研
究所内

(72)発明者 泰地 真弘人
東京都港区南麻布4-6-7 統計数理研
究所内